Appln No. 09/892,242
Amdt date September 9, 2005
Reply to Office action of July 11, 2005

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A cryptography engine for performing cryptographic operations on a data block, the cryptography engine comprising:

a key scheduler configured to provide keys for cryptographic operations;

~~multiplexer circuitry having an input stage and an output stage;~~

expansion logic coupled to the multiplexer circuitry, the expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a portion of the data block;

permutation logic coupled to the expansion logic, the permutation logic configured to alter a second bit sequence corresponding to the portion of the data block~~, whereby altering the second bit sequence performs cryptographic operations on the data block~~; and

a plurality of logic devices simulating an XOR operation for combining a key provided by the key scheduler with ~~a particular~~ the expanded first bit sequence ~~corresponding to the portion of the data block~~, the plurality of logic devices including a multiplexer receiving first and second input[[s]] values and an OR logic combining an output value of the multiplexer with a

third input value, the first, second, and third input[[s]] values being ~~derived from~~ determined based on the key provided by the key scheduler and further based on a select value indicative of whether a current cryptographic operation is to occur during an initial round of a particular series of rounds of cryptographic operations.

2. (Previously Presented) The cryptography engine of claim 1, further comprising an Sbox configured to alter a third bit sequence having a third size corresponding to the portion of the data block by compacting the third size of the third bit sequence and altering the third bit sequence using Sbox logic.

3. (Original) The cryptography engine of claim 1, wherein the cryptography engine is a DES engine.

4. (Currently Amended) The cryptography engine of claim 1[[,]] further comprising a ~~wherein the~~ multiplexer circuitry receiving initial data or feedback data from a previous round of cryptographic processing, the multiplier circuitry including ~~comprises~~ two 2-to-1 multiplexers on a first level coupled to two 2-to-1 multiplexers on a second level.

5. (Original) The cryptography engine of claim 1, wherein the first bit sequence is less than 32 bits.

6. (Original) The cryptography engine of claim 1, wherein the first bit sequence is four bits.

7. (Original) The cryptography engine of claim 5, wherein the expanded first bit sequence is less than 48 bits.

8. (Original) The cryptography engine of claim 6, wherein the expanded first bit sequence is less than six bits.

9. (Previously Presented) The cryptography engine of claim 2, wherein the third bit sequence is less than 48 bits.

10. (Previously Presented) The cryptography engine of claim 2, wherein the third bit sequence is six bits.

11. (Original) The cryptography engine of claim 9, wherein the second bit sequence is less than 32 bits.

12. (Original) The cryptography engine of claim 10, wherein the second bit sequence is four bits.

13. (Original) The cryptography engine of claim 1, wherein the key scheduler performs pipelined key scheduling logic.

14. (Original) The cryptography engine of claim 1, wherein the key scheduler comprises a plurality of stages.

15. (Original) The cryptography engine of claim 1, wherein the key scheduler comprises a determination stage.

16. (Original) The cryptography engine of claim 1, wherein the key scheduler comprises a shift stage.

17. (Original) The cryptography engine of claim 1, wherein the key scheduler comprises a propagation stage.

18. (Original) The cryptography engine of claim 1, wherein the key scheduler comprises a consumption stage.

19. (Previously Presented) The cryptography engine of claim 1, wherein a first shift amount for a first key is identified in a determination stage using a first round counter value.

20. (Currently Amended) The cryptography engine of claim 1[[,]] further comprising ~~wherein the multiplexer circuitry is~~ a two-level multiplexer receiving initial data or feedback data from a previous round of cryptographic processing.

21. (Previously Presented) The cryptography engine of claim 20, wherein the two-level multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to the output stage of the multiplexer.

22. (Original) The cryptography engine of claim 1, wherein the expansion logic and the permutation logic are associated with DES operations.

23. (Currently Amended) An integrated circuit layout associated with a cryptography engine for performing cryptographic operations on a data block, the integrated circuit layout providing information for configuring the cryptography engine, the integrated circuit layout comprising:

a key scheduler configured to provide keys for cryptographic operations;

~~multiplexer circuitry having an input stage and an output stage;~~

expansion logic coupled to the multiplexer circuitry, the expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a portion of the data block;

permutation logic coupled to the expansion logic, the permutation logic configured to alter a second bit sequence corresponding to the portion of the data block~~, whereby altering the second bit sequence performs cryptographic operations on the data block~~; and

a plurality of logic devices simulating an XOR operation for combining a key provided by the key scheduler with ~~a particular~~ the expanded first bit sequence ~~corresponding to the portion of the data block~~, the plurality of logic devices including a multiplexer receiving first and second input[[s]] values and an

OR logic combining an output value of the multiplexer with a third input value, the first, second, and third input[[s]] values being ~~derived from~~ determined based on the key provided by the key scheduler and further based on a select value indicative of whether a current cryptographic operation is to occur during an initial round of a particular series of rounds of cryptographic operations.

24. (Previously Presented) The cryptography engine of claim 23, further comprising an Sbox configured to alter a third bit sequence having a third size corresponding to the portion of the data block by compacting the third size of the third bit sequence and altering the third bit sequence using Sbox logic.

25. (Original) The cryptography engine of claim 23, wherein the cryptography engine is a DES engine.

26. (Currently Amended) The cryptography engine of claim 23[[,]] further comprising a ~~wherein the~~ multiplexer circuitry receiving initial data or feedback data from a previous round of cryptographic processing, the multiplier circuitry including ~~comprises~~ two 2-to-1 multiplexers on a first level coupled to two 2-to-1 multiplexers on a second level.

27. (Original) The cryptography engine of claim 23, wherein the first bit sequence is four bits.

28. (Original) The cryptography engine of claim 27, wherein the expanded first bit sequence is less than six bits.

29. (Original) The cryptography engine of claim 23, wherein the key scheduler performs pipelined key scheduling logic.

30. (Original) The cryptography engine of claim 23, wherein the key scheduler comprises a determination stage.

31. (Original) The cryptography engine of claim 23, wherein the key scheduler comprises a shift stage.

32. (Original) The cryptography engine of claim 23, wherein the key scheduler comprises a propagation stage.

33. (Original) The cryptography engine of claim 23, wherein the key scheduler comprises a consumption stage.

34. (Previously Presented) The cryptography engine of claim 23, wherein a first shift amount for a first key is identified in a determination stage using a first round counter value.

35. (Currently Amended) The cryptography engine of claim 23~~, wherein the multiplexer circuitry is~~ further comprising a two-level multiplexer receiving initial data or feedback data

from a previous round of cryptographic processing.

36. (Previously Presented) The cryptography engine of claim 35, wherein the two-level multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to the output stage of the multiplexer.

37. (Original) The cryptography engine of claim 23, wherein the expansion logic and the permutation logic are associated with DES operations.